AIR WAR COLLEGE

AIR UNIVERSITY

ARMY CYBER STRUCTURE ALIGNMENT

by

Brett J. Riddle, LTC, U.S. Army

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Mr. Michael Ivanovsky

16 February 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Table of Illustrations

Biography

LTC Brett Riddle entered the United States Army from Fort Benton, Montana and graduated from Montana State University in 1995. He was commissioned a Signal Officer with an Infantry branch detail assignment and attended Infantry Officer Basic Course. His first assignment was Baumholder, Germany where he deployed to Bosnia as a member of the Implementation Force (IFOR) and Stabilization Force (SFOR3) rotations. In 1998, he completed Signal Officer Branch Qualification Course and was assigned to Fort Hood, Texas where he held multiple leadership positions including company command and participated in deployments to Afghanistan and Iraq in support of Operations Enduring and Iraqi Freedom. He was accepted for branch transfer into the Functional Area 53, Information Systems Management career field in 2008, and served as the 1st Cavalry Division's and III Corps' senior automation officer. Following his Fort Hood assignments he was stationed to Brussels, Belgium and worked as the Information System Manager for U.S. Military Representative (US MILREP) to the North Atlantic Treaty Organization (NATO) Military Committee, NATO Headquarters. He is presently assigned to the Air War College at Maxwell Air Force Base, Alabama.

Abstract

The U.S. Army continues to adapt the cyber force organizational structure and roles and responsibilities to meet the strategic goals defined by Department of Defense (DoD) and U.S. Cyber Command (USCYBERCOM). The current understanding and definition of cyberspace leaves little doubt that the current structures, roles and responsibilities are insufficient to fully gain situational awareness and operational control of the domain unless changes are made. Each of the services' decisions to structure cyber forces was influenced foremost by the need to address service-specific cyber mission requirements, but was significantly constrained by internal bureaucratic priorities and organizational cultures that limited the holistic approach required to achieve unity of effort. This paper will evaluate the current missions and organizational relationships, roles, and responsibilities of USCYBERCOM and each of the supporting service's cyber component commands in order to determine whether or not the U.S. Army's current cyber structure is properly aligned to meet strategic objectives. I will conclude the paper with recommendations on how the U.S. Army can take advantage of organizational changes to align cyberspace responsibilities and authorities.

Introduction

Information technology has greatly enhanced the capability of the US military over the last thirty years, enabling tactical and operational successes since the first Gulf War. The ability to globally connect and share information nearly in real time increases the military's effectiveness and reliance on technology. The importance of protecting technological capability has been confirmed by the creation of new military cyber command structures that prioritize and synchronize the protection of Defense Department networks across the services.[1] U.S. Cyber Command (USCYBERCOM) was created in response to growing cybersecurity threats, but the idea was solidified in 2008 after a thumb drive found in a parking lot released malware that infected computers on the Department of Defense's (DoD) classified and unclassified networks, revealing how unprepared the DoD was for cyber threats.[2] Lessons learned after the thumb drive incident became the catalyst that led to the creation of a subunified USCYBERCOM under U.S. Strategic Command (USSTRATCOM) and the subsequent establishment of cyber component commands for all of the services, designated to merge their capabilities for cybersecurity and cyber operations under one command. Each of the services had different approaches to organizing and held separate views on how to build the cyber structure, which were influenced heavily by each service's organizational culture and bureaucratic tendencies. Each service wrestled with how to define cyberspace and determine which elements should be integrated into new cyber commands to provide appropriate oversight and synchronization without increasing monetary and personnel costs. Clear definitions would have to be developed to ensure that all the services understood cyberspace and how each would function to support operations. *Joint Publication 3-12, Cyber Space Operations*, defines cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology

infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[3] The *Joint Publication* also defines cyberspace operations as "the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace.[4] Such operations include computer network operations and activities to operate and defend the Global Information Grid."[5] The creation of USCYBERCOM and insertion of supporting services into the cyber organizational architecture introduced the problem of overlapping command and authority, which blurred cyber roles and responsibilities between different service commands and supporting agencies. The U.S. Army has positioned itself to meet the challenges by erecting a new cyber command built to operate and defend all U.S. Army networks, but lacking the authority and formal relationships to ensure unity of effort to accomplish cyber operations that extend beyond the command's responsibilities. This paper will evaluate the current missions and organizational relationships, roles, and responsibilities of USCYBERCOM and each of the supporting service's cyber component commands in order to determine whether or not the U.S. Army's current cyber structure is properly aligned to meet organizational strategic objectives. I will conclude the paper with recommendations on how the U.S. Army can take advantage of organizational changes to align cyberspace responsibilities and authorities.

US Cyber Command (USCYBERCOM)

USCYBERCOM was established in June 2009 as a subunified command under USTRATCOM. Its mission is to plan, coordinate, integrate, synchronize, and conduct activities to "direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the

same to our adversaries."[6] USCYBERCOM is the lead agency for coordinating, synchronizing, and directing global cyber operations and resources in coordination with the Combatant Commands (CCMDs), Joint Staff, and Office of the Secretary of Defense and ensures freedom of movement within cyberspace.[7] The commander of USCYBERCOM is also the director of the NSA and is located at Fort Meade, Maryland. USCYBERCOM also has operational command relationships with each of the services' cyber components that include: Army Cyber Command/Second Army (ARCYBER), Air Forces Cyber/24th Air Force (AFCYBER), Fleet Cyber Command/Tenth Fleet (FLTCYBERCOM), Marine Forces Cyberspace Command (MARFORCYBER), and a support relationship with service components' intelligence organizations. The Secretary of Defense authorized a recent change to the cyber structure by establishing Joint Force HQs Department of Defense Information Networks (JFHQ DODIN) under operational control of USCYBERCOM with the primary mission of managing the daily operations and defense of DoD networks.[8] USCYBERCOM continues to build its workforce with plans to complete the cyber force structure by creating 133 Cyber Mission Force (CMF) teams organized into four categories: (1) the National Mission Teams, focused on defending US national interests; (2) the Cyber Protection Teams with a mission to defend DoD networks and systems; (3) the Combat Mission Teams that will support CCMDs by integrating cyberspace effects into operational plans; and (4) Support Teams, which provide analytical and support functions to the other CMF teams.[9] USCYBERCOM does not have the capacity to staff, train, and equip the teams, and relies on each service to source and train members of the cyber force. Unsynchronized activities by the services create a disparate and service-unique approach to cyber space operations that may not align with the joint cyber vision. USCYBERCOM has mitigated the problem by developing joint-level exercises and certification programs that address

standards, but don't formally address the services' dissimilar resourcing and policy authorities, whom USCYBERCOM requires to align the cyber force structure into a cohesive and synchronized organization. Aligning policy and resourcing is only part of the problem, as the real challenge will be integrating the CMF teams into the command structure and changing the military's cultural view of technology, which is primarily viewed as a support function, and not an operational command activity. The current military culture views technology as a mission enabler, with radios and satellites supporting operations. The arrival of the CMF teams will counter the culture of technology support by forcing commands to view cyberspace as an operational effect that is a supported mission.[10]

Second Army/Army Cyber Command (ARCYBER)

On October 1, 2010, the U.S. Army created the Second Army and established Army Cyber Command (ARCYBER) in response to the Secretary of Defense's direction that all services establish a cyber command in support of USCYBERCOM's mission and operate as the service component in support.[11] ARCYBER's missions are to plan, coordinate, integrate, synchronize, direct, and conduct network operations and defense of all U.S. Army networks and to conduct cyberspace operations in support of full-spectrum operations to ensure freedom of action in cyberspace for the United States and its allies, and to deny the same to our adversaries.[12] The creation of ARCYBER as a three star service component command enabled organizational and operational control of subordinate units. ARCYBER is directly responsible for all cyberspace operations for the U.S. Army. The formation and insertion of ARCYBER into the established organizational structure addressed unity of command concerns, but created overlaps of cyber defense responsibilities with the U.S. Army's chief information officer/G6 (CIO/G6). ARCYBER has operational control over three subordinate organizations: (1) the

Network Enterprise Technology Command (NETCOM), (2) First Information Operations (IO) Command (Land), and (3) the 780th Military Intelligence (MI) Brigade. It is important to note that ARCYBER also has an important support relationship with the US Army Intelligence and Security Command (INSCOM) that maintains an administrative relationship with the 780th MI Brigade and the First IO Command.[13] INSCOM is not a subordinate operational command, but provides an essential role in supporting ARCYBER's mission.

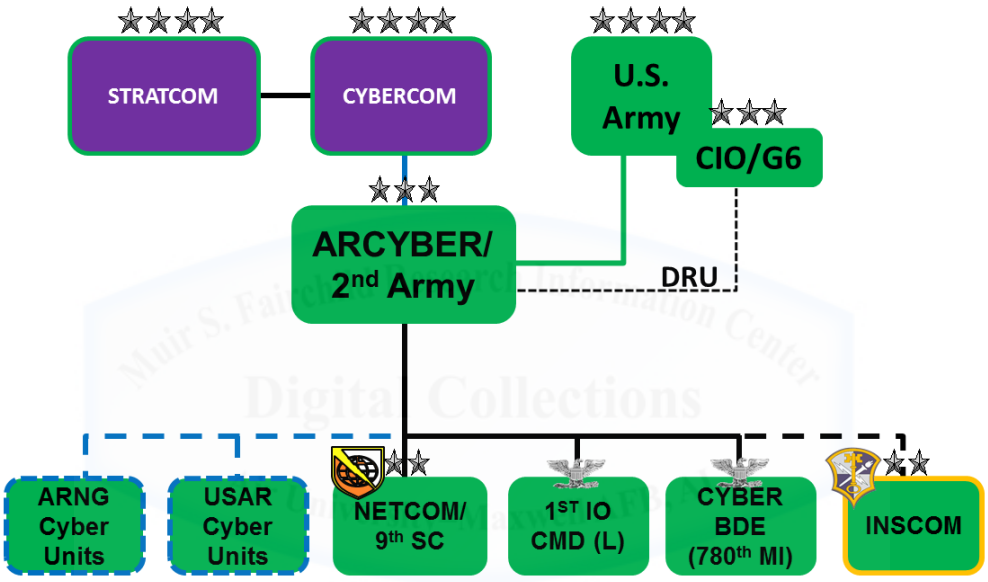

Figure 1. Army cyber command relationship.

In March 2014, the Secretary of the Army affirmed the service's commitment to unity of command in cyberspace operations by publishing *General Order 2014-02* designating ARCYBER an U.S. Army Component Headquarters commanded by a Lieutenant General and reactivating the Second Army as a Direct Reporting Unit (DRU) to the Army's Chief Information Officer/G6 (CIO/G6) and giving the commander of ARCYBER a dual responsibility as the commander of the Second Army.[14] *General Oder 2014-02* also authorizes the Second Army to carry out functions assigned to the secretary of the Army in Titles 10, 40, and 44 of the

US Code.[15] The DRU relationship between CIO/G6 and Second Army/ARCYBER aligns the cyber operational capability with the signal resources, governance, and Army policy. The mission of the Army CIO/G6 is to lead army network modernization, and to deliver timely, trusted, and shared information for itself and its mission partners.[16] The CIO/G6 authorizations are covered by USC Titles 10, 40, and 44, and reports to the Secretary of the Army in the role of Army CIO. Under this CIO capacity, the CIO supervises and manages the army's enterprise IT architecture, providing oversight for a $10 billion IT budget.[17] As the U.S. Army G6, the position is responsible for implementing information assurance and cybersecurity activities and publishing U.S. Army regulations that set cybersecurity standards for the service. ARCYBER and CIO/G6 cybersecurity authorizations and functions begin to blur and become a more prevalent issue as ARCYBER shifts focus from personnel and structure priorities to operational objectives and responsibilities. In 2011, the inability of USCYBERCOM to "see" the entire DoD network and the risks to it prompted the creation of the Joint Information Environment (JIE),[18] which is designed to consolidate and realign the departments' networks and IT systems.[19] As ARCYBER gains situational awareness and capability, the need for more centralized operational oversight will conflict with the Army's current decentralized oversight and require more clarification on the roles and responsibilities of cybersecurity activities. The Army's achievement of cyber unity of command has been primarily achieved by formalizing operational relationships with subordinate units that perform primarily cyber tasks. The introduction of ARCYBER into an established, decentralized IT infrastructure created overlaps of responsibility with the Army's CIO/G for defensive cybersecurity policy and resourcing that may counter or desynchronize ARCYBER efforts for the service. Achieving complete cyber unity of command will require

adjustments to the current DRU relationship that aligns cyber operations and resourcing with command priorities and objectives.

Twenty-Fourth Air Force/AFCYBER

On August 18, 2009, the U.S. Air Force officially activated the Twenty-Fourth Air Force to lead the service in providing full spectrum cyberspace capabilities.[20] The mission of the Twenty-Fourth Air Force is "to operate, extend, and defend the Air Force Information Network, defend key mission systems, and provide full spectrum cyberspace capabilities for the joint warfighter."[21] AFCYBER has operational control over three subordinate units: (1) the Sixty-seventh Network Warfare Wing, (2) 688th Information Operations Wing, and (3) the Fifth Communications Combat Group.[22]

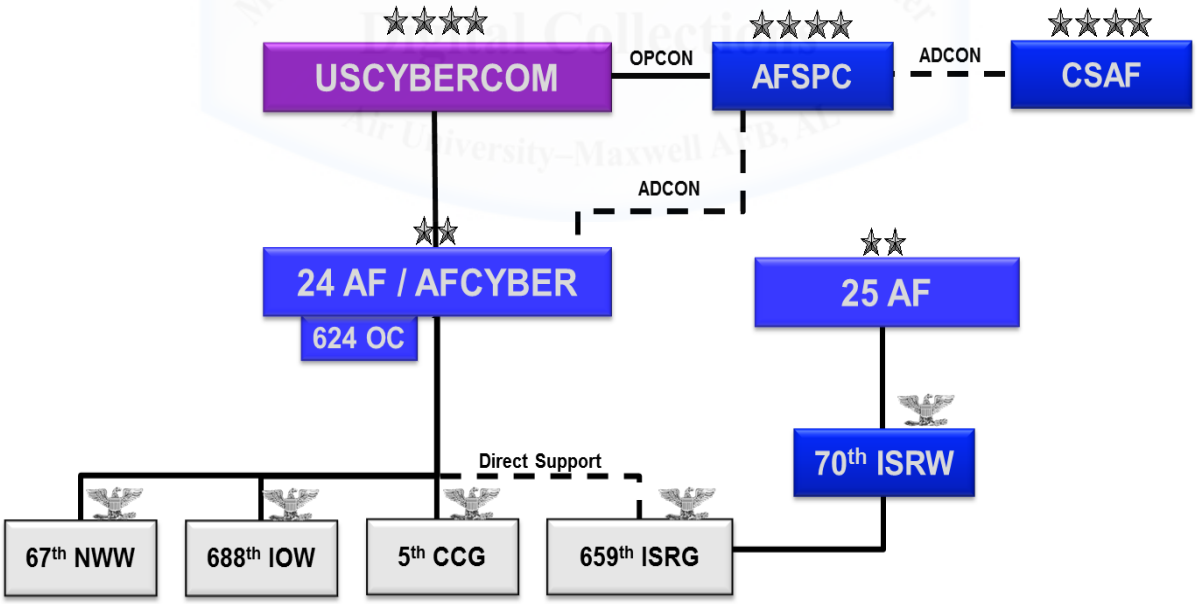

Figure 2. Air Force cyber command relationship.

On August 20, 2009, the secretary and Chief of Staff of the Air Force published a memo on cyberspace mission alignment that designated Air Force Space Command (AFSPC) as lead

USAF major command for the cyberspace mission and also established Twenty-Fourth Air Force/AFCYBER as the service component representative to USCYBERCOM, aligning authorities and responsibilities to enable seamless cyberspace operations.[23] The authorizations for the U.S. Air Force cyber forces are the same as those of the U.S. Army cyber forces, which are governed by USC Titles 10, 50, and 32 for the National Guard, but unlike the U.S. Army, the U.S. Air Force CIO/A6 does not have a formal command relationship with AFCYBER or Air Force Space Command (AFSPC). This is an interesting point, because both elements have a shared oversight in providing cybersecurity for the U.S. Air Force. AFSPC is designated as the lead command for all U.S. Air Force cyber operations via the Twenty-Fourth/AFCYBER and is the focal point for defense, attack, exploitation, and operations.[24] The U.S. Air Force CIO/A6 has overall responsibility for cybersecurity, developing IT policies, program resources, and cyberspace operations.[25] The only official cybersecurity connection between the two organizations is a situational report that AFSPC has been tasked to provide to the U.S. Air Force CIO/A6 that covers information on the operational status and network health of the globally interconnected capabilities.[26] The lack of a formal command relationship may inhibit communication between the staff elements and desynchronize efforts over time. The informal relationship is dependent on priorities and how much energy can be focused on maintaining communication.

Another distinction between the Air Force's cyber organizational structure and the Army's is the Intelligence, Surveillance and Reconnaissance (ISR) relationships with each of the cyber commands. The Air Force's 659th Intelligence, Surveillance and Reconnaissance Group (ISRG) has a support relationship with AFCYBER, while ARCYBER has operational control of cyber intelligence units within the 780th MI Brigade. The 659th remains under operational control

of the 70th ISRW and must support both missions between two different commands. Prioritizing resources, training, and mission tasks may become problematic for an organization that must respond to two different commands. The Air Force chief of staff published a memo on July 7, 2015, announcing an initiative to integrate the cyberspace and ISR/EW capabilities through a virtual partnership between the Twenty-Fourth and Twenty-Fifth Air Force that incorporates subject-matter experts from different fields, including academia, the National Intelligence community, and the Air Force Life Cycle Management Center.[27] The memo signifies how detached the ISR/EW and cyberspace communities have become under the current support relationships and may indicate that future changes will be required to formally establish operational control of the 659th under the Twenty-Fourth Air Force/AFCCYBER.

Navy Fleet Cyber Command/Tenth Fleet (FLTCYBERCOM)

The U.S. Navy adopted a holistic approach when determining how to assemble its cyber force structure, and in October of 2009 it consolidated the Office of Navy Intelligence (N2) and the Communications Network Directorate (N6) into the N2/N6 Information Dominance Corps. The purpose of the consolidation was to increase the importance of information and elevate it to a core U.S. Navy warfighting capability by integrating intelligence, information warfare, and information/network management operations to improve command and control and information access for the operational forces.[28] The creation of Information Dominance Corps and the N2/N6 was a significant step in acknowledging the U.S. Navy's technological interdependencies and the importance of defending capabilities by uniting the different communities that contribute to cyberspace operations.

The mission for the N2/N6 is to provide effective, efficient, trusted, and shared information management/information technology (IM/IT) and information resource management (IRM) enterprise capabilities to support the Navy, its marines, sailors, and their mission partners in conducting global military and business operations.[29] Consolidating the N2/N6 and cyber priorities within the Information Dominance Corps' overall strategy sends a clear message that the Navy's leadership is taking steps to ensure that cyberspace equities are prioritized and have the proper oversight for future development. Shortly after the consolidation of the N2/N6, the Chief of Naval Operations (CNO) established FLTCYBERCOM/Tenth Fleet on January 29, 2010, as the Navy Component Command (NCC) to USCYBERCOM and USSTRATCOM, to serve as the central operational authority for networks, cryptologic and signals intelligence (SIGINT), information operations (IO), cyber, electronic warfare (EW), and space capabilities in support of forces afloat and ashore.[30] The Tenth Fleet is solely responsible for evaluating U.S. Navy cyberspace operations and organizes, trains, and equips all forces under its command. Having a single cyber authority over multiple capabilities aligns efforts toward a single mission and decreases friction and conflict over assigned roles and responsibilities. The FLTCYBERCOM/Tenth Fleet mission is to serve as the Numbered Fleet for Fleet Cyber Command and to exercise operational control of assigned naval forces to coordinate with other naval, coalition, and joint task forces to execute the full spectrum of cyber, electronic warfare, information operations, and signal intelligence capabilities and missions across the cyber, electromagnetic, and space domains.[31]

The inclusion of cryptologic, SIGINT, and cyberspace capabilities within the FLTCYBERCOM and the Information Dominance Corps umbrella provides the U.S. Navy distinctive capabilities by aligning the different activities organizationally, taking advantage of

unity of command efforts that increase operational exploitation capabilities and collaboration within the organization. The commander owns the cyber intelligence assets and can prioritize and redirect them when required. The inclusion of SIGINT also expands FLTCYBERCOM authority by adding USC Title 50 to Title 10 capacities that would normally have to be coordinated through a separate agency. Signals Intelligence (SIGINT) operations under Title 50 are authorized to analyze the network activity of targeted users and or computers, analyze network activity of targeted groups, provide alerts when targeted users/computers are active, track network usage, and determine associations of groups and individuals.[32]

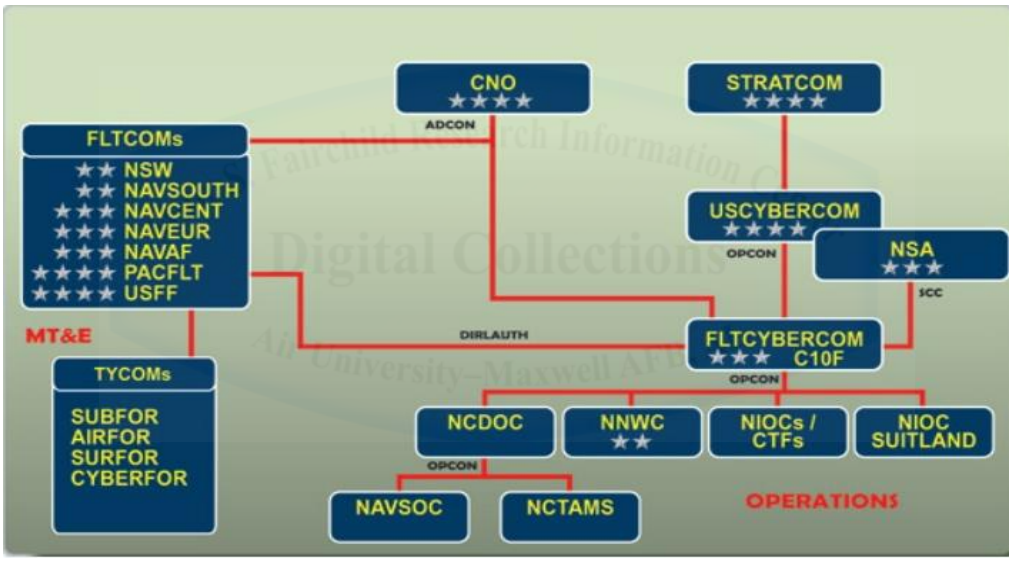

Figure 3. Navy cyber command relationship.

Each organization supporting cyberspace operations is aligned to one or more lines of operation within the Information Dominance Corps strategy. The Navy's holistic cyberspace organizational approach ensures unity of command benefits and closely aligns organizational responsibilities with authority, providing the commander with the tools and resources to effectively accomplish missions.

US Marine Force Cyber Command (MARFORCYBER)

The U.S. Marine Corps (USMC) established MARFORCYBER in October 2009 and has the smallest service component command under USCYBERCOM, with fewer than 300 military and civilian personnel.[33] MARFORCYBER's mission is to "plan, coordinate, integrate, synchronize, and direct our Corps' full spectrum of cyberspace operations."[34] This includes DoD information network (DoDIN) operations, defensive cyber operations (DCO), and planning and, when required, executing offensive cyberspace operations.[35]

The MARFORCYBER units support the global mission of the Marine Corps, Marine Air Ground Task Force (MAGTF), joint and combined cyberspace requirements that enable freedom of action across all warfighting domains and deny the same to adversarial forces.[36] Lt. Gen. George Flynn, the deputy commandant commanding the Marine Corps Combat Development Command at the time, stated the marines' cyber role was to ensure defense of the corps and DoD. "If we are to be dominant on land, at sea, and in the air, we must be dominant in cyberspace,"[37] MARFORCYBER has two subordinate organizations: (1) Marine Corps Network Operations Security Center (MCNOSC), which provides IT services, networks, and governance; and (2) Marine Corps Cyberspace Warfare Group (MCCYWG), which provides Title 10 full-spectrum cyberspace capabilities in support of USMC requirements. In a support role, the Marine Corps Information Operations Center (MCIOC) provides information operations resources and activities to MARFORCYBER when requested.

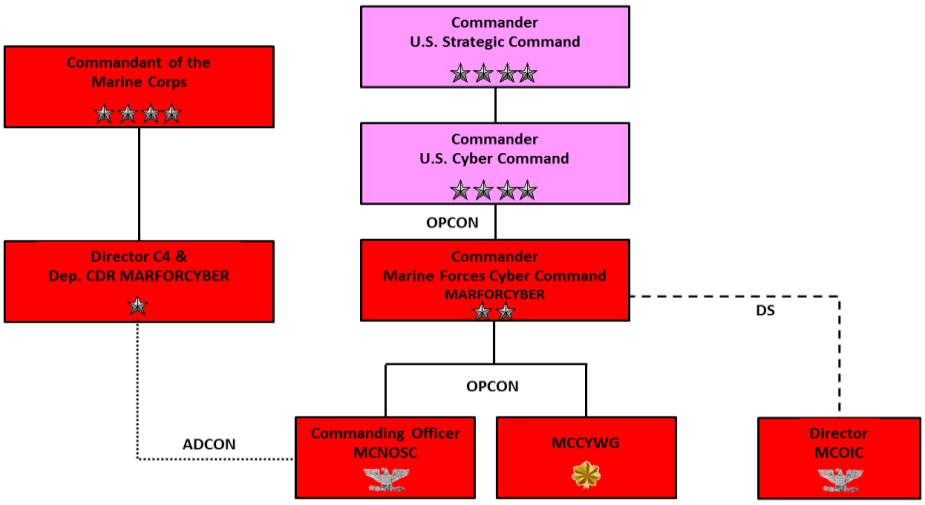

Figure 4. Marine Corps cyber command relationship.

The roles and responsibilities of USMC cyberspace operations are similar to the U.S. Army's and U.S. Air Force's, but are structured differently at the service headquarters level. The Deputy Commandant for Plans, Policies and Operations (DC, PP&O), serves as the lead advocate for cyberspace operations, providing advice and recommendations to the commandant on cyberspace issues.[38] The Director, Command, Control, Communications, and Computers (C4) and CIO, also has the role of the deputy commander for MARFORCYBER. This consolidation strengthens the relationship between the IT services and defense and cybersecurity operations. In the CIO role, is charged with providing IT capital planning and portfolio management, developing and managing the IT architecture and workforce, and providing leadership and governance of IT activities for USMC. [39] In the Deputy Commander role, provides coordination and develops strategies and plans to ensure all marines can conduct operations through shared, secured, and reliable environments. The Director of Intelligence is tasked with developing plans and policy for the conduct of intelligence and counterintelligence activities in support of cyberspace operations in concert with undersecretary of defense for intelligence, the office of the director of national intelligence, and joint intelligence plans and policy.[40] The USMC

acknowledges that its organizational approach using an operational advocate and intra-staff coordination has been problematic, and recently formed Task Force Cyber to address the problems. Colonel Gregory Breazile, Commanding Officer, Marine Corps Communication-Electronics School, stated, "We've got organizational issues, we've got command and control issues, we've got acquisition issues, we've got manpower and training issues. Across the entire capability of cyberspace operations we've got issues."[41] Task Force Cyber's objective is to collect all of the issues and make recommended changes to USMC's Combat Development Command.[42]

Recommendations

Each of the services' decisions to structure cyber forces was influenced foremost by the need to address service-specific cyber mission requirements, but was significantly constrained by internal bureaucratic priorities and organizational cultures that limited the holistic approach required to achieve unity of effort. Availability of money and human resources are two major factors that contributed to the limited approach and have forced the services to build new structures using existing resources, thereby constraining the ability to appropriately build out the cyber force structure. Each of the services dug in to protect its organizational resources and priorities, not fully committing to an all-inclusive solution to cyber force development. The broad scope of cyberspace as defined by *Joint Publication 3-12* leaves little doubt that the current structures, roles, and responsibilities are insufficient to fully gain situational awareness and operational control of the domain unless changes are made. Lt. Gen. Cardon, ARCYBER Commander, stated in testimony to the House Armed Services Committee on Emerging Threats and Capabilities that recent intrusions clearly underscore the extent that DoD lacks sufficient situational awareness, putting operations and sensitive data at great risk.[43] The current resource-

constrained environment is unlikely to change in the foreseeable future, but there are changes that the Army can undertake to align cyberspace operations and unity of effort.

The first step the U.S. Army should explore to increase cyberspace operations unity of effort is merging the G2 and G6 positions into one staff element, mirroring the U.S. Navy's consolidation of the N2/N6 positions. This consolidation will align cyber intelligence capabilities with defensive network operations at the department headquarters level, synchronizing resourcing and policy development for a unified cyber front. Combining the two staff elements removes bureaucratic boundaries, increases flexibility in decision-making, and improves collaboration between the intelligence and IT services communities, enabling resource prioritization and policy development. Starting structural changes at the top level ensures integration of cyber priorities and will facilitate further integration at the tactical level.

A subsequent step needed to complement G2/G6 consolidation to increase unity of effort is to change the command relationship between ARCYBER and INSCOM from a supporting one to an operational control relationship, mirroring the DRU relationship between NETCOM and ARCYBER. A DRU relationship would be created between ARCYBER and the Army G2, matching the DRU relationship that currently exists between ARCYBER and the Army CIO/G6 to synchronize intelligence resourcing and policy development. The change would bring both NETCOM and INSCOM under operational control of ARCYBER, thus enhancing the holistic approach that the domain requires. The change would also facilitate streamlining the Title 10 and Title 50 authorizations for the command by providing ARCYBER with the appropriate service cryptologic component designation to conduct Title 50 activities internally. Lt. Gen. Cardon stated in his testimony to the House Armed Services Committee on Emerging Threats and Capabilities that "achieving operational success hinges on having the requisite command and

control, alignment of authorities with missions, and other key enabling capabilities such as intelligence, targeting information technology and communication activities."[44] ARCYBER is tasked with the operational lead for cyberspace operations; aligning Title 10 and 50 authorizations will ensure that capabilities match responsibilities. Changing the command relationship between INSCOM and ARCYBER will strengthen INSCOM's other intelligence disciplines (HUMINT, GEOINT, MASINT, etc.), which are dependent on cyberspace capabilities, by removing bureaucratic barriers that inhibit decision processes and desynchronize capabilities.

A second area where the U.S. Army can align to improve cyber synchronization is adopting a holistic approach to training. The convergence of cyber intelligence and cyber operations blurs the line of separation between existing traditional training structures and will have to be closely monitored to ensure that warfighters and strategic commands receive soldiers who are properly trained to meet mission requirements. The U.S. Army has taken a positive first step by designating Fort Gordon as the Cyber Center of Excellence, described by Lt. Gen. Cardon as "the Army's center of gravity for institutionalizing cyberspace, to include developing the necessary doctrinal, organizational, training, and materiel activities and policies."[45] A logical next step could include developing a formal training partnership between the Cyber and Intelligence Centers of Excellence to deconflict areas that overlap and strengthen identified supporting activities between the two organizations. Maj. Gen. Stephen Fogarty, the commander of the Army Cyber Center of Excellence, stated, "the reality is [intelligence and cyberspace] are not connected in the way we need to be."[46] Cyberspace enables intelligence and intelligence enables cyberspace operations. A training partnership will benefit not only both organizations, but the entire U.S. Army with clear, concise, and relevant doctrine that is coordinated and

synchronized. The integration of cyber forces into tactical formations has revealed huge gaps in knowledge about cyber capabilities. The Twenty-Fifth Infantry Division participated in a cyber pilot training program during its National Training Center rotation, and the commander's key observation was summed up when he stated, "The policies, permissions and authorities are not changing at the speeds relative to the threats; the skills are not developing at the speed relative to threats; commanders' awareness in broad terms remains to be lacking and a big change in command for communications and cyber remain confusing across the force."[47] The echelons corps and below have yet to understand the importance of cyberspace operations and how to integrate cyberspace effectively into the mission. Lack of cyber force structure and human resources at the tactical level is partly to blame, but developing a holistic approach to cyber training that expands to other branches will help resolve some of the confusion. A holistic-training approach will acknowledge the expansive dependencies that military war fighting systems have on technology and ensure they have the knowledge to degrade an opponent's cyber capabilities simultaneously.

The cyber training pilot program identified cyber-training gaps, but also highlighted the matter of how cyber operations are perceived throughout the force. Historically, IT systems, telecommunications, and network defense functions have been viewed as supporting or tertiary efforts, to be focused on only when problems affect operations, usually negatively. Given the technical nature of the problems, the warfighters relied exclusively on the IT and communications staff to resolve issues with little oversight. The U.S. Army must change the current organizational culture and fight in the cyber domain with the same mindset that is applied to other warfighting domains. Adm. Rogers, USCYBERCOM Commander, acknowledged the importance of operationalizing cyberspace security and the need to change operational mindsets

"whereby our networks and cyber capabilities are not administered but rather led by commanders who understand they are always in real or imminent contact with adversaries."[48] The ARCYBER commander thinks the same way, and stated, "Cyber issues had been approached from either a communications perspective or an intelligence perspective—not from an operational perspective." [49]

Conclusion

The U.S. Army has taken significant steps to increase cyber capabilities by elevating ARCYBER to a service component command, creating a new cyber branch, and identifying a Cyber Center of Excellence. Much more change is required to fully address the challenges presented by cyberspace operations. The U.S. Army needs to embrace a holistic, unity of effort approach at all levels, which will require organizational changes and force structural changes. The understanding and influence of cyber operations will only grow as the services' dependencies on technology grow and expand to the lowest ranks of soldiers. Responsibility for the defense of cyberspace overlaps different branches, creating confusion and gaps at the organizational and cultural levels. Changing the cyberspace organizational structure to align responsibilities with authority will strengthen the U.S. Army's overall mission capabilities and will help clarify the role of cyberspace operations at the tactical level.

Endnotes

[1] Tom Burghardt, *The Launching of U.S. Cyber Command (CYBERCOM)*, *Global Research*, 30 June 2009, (accessed 14 February 2016), http://www.globalresearch.ca/the-launching-of-u-s-cyber-command-cybercom/14186.

[2] Ellen Nakashima, *Cyber-Intruder Sparks Response, Debate*, *The Washington Post*, 8 December 2011, (accessed on 14 February 2016), https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html .

[3] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12, (Washington, DC: U.S. Joint Chiefs of Staff, 5 February 2013), V.

[4] Ibid., II-1.

[5] Ibid., 99.

[6] U.S. Cyber Command (USCYBERCOM), "*USCYBERCOM Fact Sheet*," (accessed on 14 February 2016), https://www.stratcom.mil/factsheets/2/Cyber_Command/ .

[7] U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12, IX.

[8] U.S. Department of Defense (DoD), *The DoD Cyber Strategy*, April 2015, (accessed on 14 February 2016), http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, 20.

[9] Ibid., 6, 20.

[10] Mark Pomerleau, *For DOD, building the cyber force is a team game*, *Defense Systems*, 30 July 2015, (accessed on 14 February 2016), https://defensesystems.com/Articles/2015/07/30/Building-cyber-mission-force.aspx?Page=2 .

[11] United States Army Cyber Command and Second Army official website, *Establishment of U.S. Army Cyber Command*, (accessed on 14 February 2016) http://www.arcyber.army.mil/Organization/ARCYBERHistory .

[12] US Army Cyber Command, "ARCYBER the Next Battlefield," briefing slides, Ft. Meade, MD, December 10, 2013.

[13] George I. Seffers, *Historic Cyber Unit Begins Daily Action*, *Signal Magazine*, March 2012, (accessed on 14 February 2016), http://www.afcea.org/content/?q=historic-cyber-unit-begins-daily-action .

[14] John M. McHugh, Secretary of the Army, HQDA General Order 2014-02, Affirmation of Secretary of the Army commitment to unity of effort; designation of U.S. Army Cyber Command as an Army force component headquarters, March 2014, 1.

[15] Ibid., 2.

[16] Department of the Army Chief Information Officer/G6 (CIO/G6), official website, Enabling Success, Mission Statement, (accessed on 14 February 2016), http://ciog6.army.mil/AboutCIO/Mission/tabid/62/Default.aspx .

[17] LTG Robert Ferrell, Office of the Chief Information Officer, "Army CIO/G6 Overview," briefing slides, Pentagon, Washington DC, September 2014.

[18] Gary W. Blohm, *U.S. Army – Network Security Enterprise Reference Architecture*, Department of the Army CIO/G-6 Enterprise Reference Architecture Series, Version 2.0 29 September 2014, 2.

[19] Department of Defense, *The Department of Defense Strategy for Implementing the Joint Information Environment*, "Response to Section 931(a) of the Fiscal Year 2013 National Defense Authorization Act (NDAA)," September 18, 2013, (Executive Summary).

[20] Tech. Sgt. Scott McNabb, *24th AF becomes AFCYBER*, Air Force Public Affairs Office, 7 December 2010, (accessed on 14 February 2016), http://www.24af.af.mil/news/story.asp?id=123233885 .

[21] 24th Air Force/AFCYCBER, *24th Air Force Fact Sheet*, 24th Air Force Public Affairs, 11 June 2014, (accessed on 14 February 2016), http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663 .

[22] Ibid.

[23] Secretary of the Air Force Michael B. Donley and Chief of Staff of the Air Force Gen. Norton A. Schwartz, "Air Force Cyberspace Mission Alignment," memorandum for all Airmen, Washington, DC, 20 August 2009.

[24] Headquarters Air Force Space Command, Air Force Space Command Instruction 90-102, *AFSPC Organizational Roles, Authorities, and Relationships*, 16 June 2011, 11.

[25] Secretary of the Air Force, HAF Mission Directive 1-26, *Chief, Information Dominance and Chief Information Officer*, 5 February 2015, 1,6.

[26] Secretary of the Air Force, Air Force Instruction 33-200, *Air Force Cybersecurity Program Management*, 31 August 2015, 8,22.

[27] Chief of Staff of the Air Force Gen. Mark A. Welsh III, "Cyberspace-ISR-EW Integration and Innovation," memorandum for all Major Commands, Direct Reporting Units, and Combatant Commands, Washington, DC, 7 July 2015.

[28] Director of Navy Staff Vice Admiral Sam J. Locklear, "Establishment of the Deputy Chief of Naval Operations for Information Dominance (N2/N6)," Navy Admin Message, 29 October 2009, http://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2009/NAV09316.txt.

[29] Department of the Navy Chief Information Officer, official website, DON IM/IT/Cyberspace Vision, Mission and Goals, Mission Statement, (accessed on 14 February 2016), http://www.doncio.navy.mil/ContentView.aspx?ID=649.

[30] Director of Navy Staff Vice Admiral J. M. Bird, *Missions, Functions, and Tasks of Commander, U.S. Fleet Cyber Command and Commander, U.S. Tenth Fleet*, OPNAVINST 5450.345 for Major Commands, Direct Reporting Units, and Combatant Commands, Washington, DC, 4 April 2012, 2.

[31] U.S. Fleet Cyber Command and Tenth Fleet, official website, 1 December 2010, (accessed on 14 February 2016), http://www.public.navy.mil/fcc-c10f/Pages/ustenthfleetmission.aspx .

[32] Starnes Walker, "U.S. Fleet Cyber Command, U.S. Tenth Fleet," briefing slides to AFCEA, Washington DC, April 2012, (accessed 14 February 2016), https://cryptome.org/2013/10/fcc-10th.pdf .

[33] J.R. Wilson, *MARFORCYBER: Marines Fight in a New Domain*, *Defense Media Network*, 5 January 2012, (accessed 14 February 2016) www.defensemedianetwork.com/stories/marforcyber-marines-fight-in-a-new-domain/.

[34] U.S. Marine Corps Forces Cyberspace (MARFORCYBER), official website, 11 February 2016, (accessed on 14 February 2016), https://marinecorpsconceptsandprograms.com/organizations/operating-forces/us-marine-corps-forces-cyberspace-marforcyber.

[35] Ibid.

[36] Ibid.

[37] J.R. Wilson, *MARFORCYBER: Marines Fight in a New Domain*, *Defense Media Network*

[38] Commandant Marine Corps, *Cyberspace Operations*, Marine Corps Order 3100.4, 27 July 2013,4, http://www.marines.mil/Portals/59/Publications/MCO%203100.4.pdf .

[39] Ibid., 7

[40] Ibid., 8

[41] Megan Eckstein, *Marine Corps Cyber Task Force Stood Up, Will Report to Commandant This Summer*, *USNI News*, 28 April 2015, http://news.usni.org/2015/04/28/marine-corps-cyber-task-force-stood-up-will-report-to-commandant-this-summer,

[42] Ibid.

[43] Lt. Gen. Edward C. Cardon, Lieutenant General, Commanding General U.S. Army Cyber Command and Second Army, statement before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities Operationalizing Cyberspace for the Services, First Session 114th Congress, *Congressional Record*, (4 March 2015), 9.

[44] Ibid., 3.

[45] Ibid., 2.

[46] Jared Serbu, *Army's new cyber center aims to build top-notch cyber forces, not 'exquisite stovepipes'*, *Federal News Radio*, 26 September 2014, http://federalnewsradio.com/defense/2014/09/armys-new-cyber-center-aims-to-build-top-notch-cyber-forces-not-exquisite-stovepipes/ .

[47] Jen Judson, *Army Learning How Cyber Support Plays Role In Tactical Operations*, *Defense News*, 10 November 2015, http://www.defensenews.com/story/defense/land/army/2015/11/10/army-learning-how-cyber-support-plays-role-in-tactical-operations/75545442/ .

[48] Admiral Michael Rogers, USCYBERCOM Command, *Beyond the Build Delivering Outcomes through Cyberspace, The Commander's Vision and Guidance for US Cyber Command*, 3 June 2015, 5, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf .

[49] Robert K. Ackerman, *Convergence Dominates Army Cyber Activities*, *Signal Magazine*, 1 October 2015, http://www.afcea.org/content/?q=Article-convergence-dominates-army-cyber-activities.

Bibliography

24th Air Force/AFCYCBER, *24th Air Force Fact Sheet*, 24th Air Force Public Affairs, 11 June 2014, http://www.24af.af.mil/library/factsheets/factsheet.asp?id=15663.

Ackerman, Robert K., *Convergence Dominates Army Cyber Activities*, *Signal Magazine*, 1 October 2015, http://www.afcea.org/content/?q=Article-convergence-dominates-army-cyber-activities.

Blohm, Gary W., *U.S. Army – Network Security Enterprise Reference Architecture*, Department of the Army CIO/G-6 Enterprise Reference Architecture Series, Version 2.0 29 September 2014, 2.

Burghardt, Tom, *The Launching of U.S. Cyber Command (CYBERCOM)*, Global Research, 30 June 2009, http://www.globalresearch.ca/the-launching-of-u-s-cyber-command-cybercom/14186.

Cardon, Edward C., Lieutenant General, Commanding General U.S. Army Cyber Command and Second Army, statement before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities Operationalizing Cyberspace for the Services, First Session 114th Congress, *Congressional Record*, (4 March 2015), 9.

Chief of Staff of the Air Force Gen. Mark A. Welsh III, "*Cyberspace-ISR-EW Integration and Innovation*," memorandum for all Major Commands, Direct Reporting Units, and Combatant Commands, Washington, DC, 7 July 2015.

Commandant Marine Corps, *Cyberspace Operations*, Marine Corps Order 3100.4, 27 July 2013,4, http://www.marines.mil/Portals/59/Publications/MCO%203100.4.pdf.

Department of Defense, *The Department of Defense Strategy for Implementing the Joint Information Environment*, "Response to Section 931(a) of the Fiscal Year 2013 National Defense Authorization Act (NDAA)," September 18, 2013, (Executive Summary).

Department of the Army Chief Information Officer/G6 (CIO/G6), official website, Enabling Success, Mission Statement, http://ciog6.army.mil/AboutCIO/Mission/tabid/62/Default.aspx.

Department of the Navy Chief Information Officer, official website, *DON IM/IT/Cyberspace Vision, Mission and Goals, Mission Statement*, http://www.doncio.navy.mil/ContentView.aspx?ID=649.

Director of Navy Staff Vice Admiral J. M. Bird, *Missions, Functions, and Tasks of Commander, U.S. Fleet Cyber Command and Commander, U.S. Tenth Fleet*, OPNAVINST 5450.345 for Major Commands, Direct Reporting Units, and Combatant Commands, Washington, DC, 4 April 2012, 2.

Director of Navy Staff Vice Admiral Sam J. Locklear, "Establishment of the Deputy Chief of Naval Operations for Information Dominance (N2/N6)," Navy Admin Message, 29 October 2009, http://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2009/NAV09316.txt.

Eckstein, Megan, *Marine Corps Cyber Task Force Stood Up, Will Report to Commandant This Summer, USNI News*, 28 April 2015, http://news.usni.org/2015/04/28/marine-corps-cyber-task-force-stood-up-will-report-to-commandant-this-summer.

Ferrell, Robert, LTG Office of the Chief Information Officer, "Army CIO/G6 Overview," briefing slides, Pentagon, Washington DC, September 2014.

Headquarters Air Force Space Command, Air Force Space Command Instruction 90-102, *AFSPC Organizational Roles, Authorities, and Relationships*, 16 June 2011, 11.

Judson, Jen, *Army Learning How Cyber Support Plays Role In Tactical Operations, Defense News*, 10 November 2015, http://www.defensenews.com/story/defense/land/army/2015/11/10/army-learning-how-cyber-support-plays-role-in-tactical-operations/75545442/.

McHugh, John M., Secretary of the Army, HQDA General Order 2014-02, *Affirmation of Secretary of the Army commitment to unity of effort; designation of U.S. Army Cyber Command as an Army force component headquarters*, March 2014, 1.

McNabb, Scott, Tech. Sgt., *24th AF becomes AFCYBER*, Air Force Public Affairs Office, 7 December 2010, http://www.24af.af.mil/news/story.asp?id=123233885.

Nakashima, Ellen, *Cyber-Intruder Sparks Response, Debate, The Washington Post*, 8 December 2011, https://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

Pomerleau, Mark, *For DOD, building the cyber force is a team game, Defense Systems*, 30 July 2015, https://defensesystems.com/Articles/2015/07/30/Building-cyber-mission-force.aspx?Page=2.

Rogers, Michael, Admiral, USCYBERCOM Command, *Beyond the Build Delivering Outcomes through Cyberspace, The Commander's Vision and Guidance for US Cyber Command*, 3 June 2015, 5, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf.

Secretary of the Air Force Michael B. Donley and Chief of Staff of the Air Force Gen. Norton A. Schwartz, "Air Force Cyberspace Mission Alignment," memorandum for all Airmen, Washington, DC, 20 August 2009.

Secretary of the Air Force, Air Force Instruction 33-200, *Air Force Cybersecurity Program Management*, 31 August 2015, 8,22.

Secretary of the Air Force, HAF Mission Directive 1-26, *Chief, Information Dominance and Chief Information Officer*, 5 February 2015, 1,6.

Seffers, George I., *Historic Cyber Unit Begins Daily Action, Signal Magazine*, March 2012, http://www.afcea.org/content/?q=historic-cyber-unit-begins-daily-action.

Serbu, Jared, *Army's new cyber center aims to build top-notch cyber forces, not 'exquisite stovepipes'*, Federal News Radio, 26 September 2014, http://federalnewsradio.com/defense/2014/09/armys-new-cyber-center-aims-to-build-top-notch-cyber-forces-not-exquisite-stovepipes/.

U.S. Cyber Command (USCYBERCOM), "USCYBERCOM Fact Sheet," https://www.stratcom.mil/factsheets/2/Cyber_Command/.

U.S. Department of Defense (DoD), *The DoD Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf , 20.

U.S. Fleet Cyber Command and Tenth Fleet, official website, 1 December 2010, http://www.public.navy.mil/fcc-c10f/Pages/ustenthfleetmission.aspx.

U.S. Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12, (Washington, DC: U.S. Joint Chiefs of Staff, 5 February 2013), V.

U.S. Marine Corps Forces Cyberspace (MARFORCYBER), official website, 11 February 2016, https://marinecorpsconceptsandprograms.com/organizations/operating-forces/us-marine-corps-forces-cyberspace-marforcyber.

U.S. Army Cyber Command and Second Army official website, Establishment of U.S. Army Cyber Command, http://www.arcyber.army.mil/Organization/ARCYBERHistory.

U.S. Army Cyber Command, "ARCYBER the Next Battlefield," briefing slides, Ft. Meade, MD, December 10, 2013.

Walker, Starnes, "U.S. Fleet Cyber Command, U.S. Tenth Fleet," briefing slides to AFCEA, Washington DC, April 2012, https://cryptome.org/2013/10/fcc-10th.pdf.

Wilson, J.R., MARFORCYBER: *Marines Fight in a New Domain, Defense Media Network*, 5 January 2012, www.defensemedianetwork.com/stories/marforcyber-marines-fight-in-a-new-domain/.